Блокчейн для разработчиков

Предисловие

Эта книга написана для тех, кто хочет попробовать себя в разработке децентрализованных приложений. Она будет интересна как разработчикам, так и всем тем, кто принимает непосредственное участие в подобных проектах: руководителям, инвесторам, проджект менеджерам.

В книге не будет описания разработки самого блокчейна, так как в большинстве случаев не имеет смысл создавать собственный блокчейн под приложение. Но я разберу то, как устроены существующие блокчейны, их принципы работы, особенности, плюсы и минусы, для того, чтобы вы могли понять сложности и преимущества и принять решение о необходимости использования блокчейна для своего проекта.

Мы рассмотрим, как создать приложение на блокчейне Ethereum с использованием фреймворка Truffle. Узнаем, что надо предпринять до того, как Вы начали писать приложение, затронем юридические аспекты криптовалют, определим те технологии, которые надо учитывать при написании приложения для того, чтобы оно хорошо работало.

Также я расскажу об инструментах, используемых для создания приложений. На примере простейшего приложения для голосования объясню, как написать смарт-контракт, протестировать его, а также опубликовать в блокчейне.

Введение

Что такое блокчейн?

Технология блокчейн последнее время наделала много шума. Эксперты пророчат ей великое будущее, проекты на блокчейне собирают миллионы долларов, изобретение блокчейна сравнивают с изобретением Интернета. Даже если вы никогда не слышали об этой технологии, то о Биткойне вы слышали 100%. В основе криптовалюты Биткойн как раз и лежит технология блокчейн. Попробуем разобраться, что же это такое.

Говоря сухим научным языком, блокчейну можно дать следующее определение.

*Блокчейн – это распределенная база данных, содержащая факты, называемые блоками, реплицированная на несколько компьютеров, собранных в одноранговую сеть. Участниками сети являются анонимные лица, называемые узлами. Каждый блок содержит криптографический хеш предыдущего блока, метку времени и данные транзакциии. Добавление фактов в базу происходит только на основании консенсуса. Данные из блокчейна удалить нельзя.*

Сложно для понимания, но к концу книги вы поймете, о чем речь.

Децентрализованные сети, которыми по сути и являются блокчейны, не новы в мире информационных технологий. Создание децентрализованных сетей началось намного раньше, чем вся эта шумиха с криптовалютами. Достаточно вспомнить о таких децентрализованных одноранговых сетях (их еще называют пиринговыми или P2P сетями), как BitTorrent или Napster, участники которых использовали сеть для обмена фильмами. Так в чем же отличие и ценность блокчейна? В чем была необходимость его создания? Какую проблему он должен решить? И нужен ли вообще блокчейн для вашего проекта? Попробуем разобраться.

Часть 1. Теория

В этой части я расскажу о том, как возник блокчейн, как он работает и где его можно использовать. Я помогу вам определиться, действительно ли для вашего проекта необходима блокчейн технология или же можно обойтись известными проверенными альтернативными решениями. Помните, что неграмотное или неуместное использование блокчейна скорее оттолкнет от вашего проекта, чем привлечет к нему внимание.

Глава 1. Значимость технологии блокчейн для современного мира.

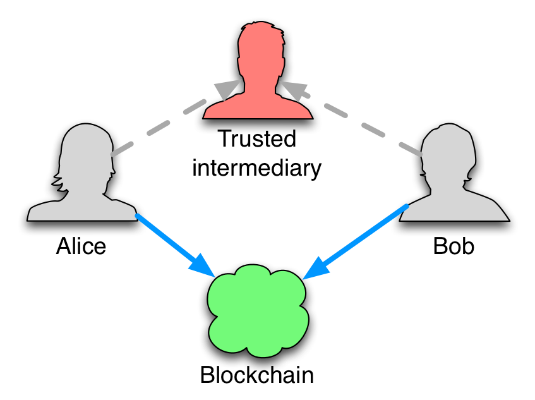
Современная экономика переживает трансформацию и постепенно уходит из реального мира в цифровой. Данный процесс принято назвать цифровой трансформацией. Этот процесс непрерывно связан с оптимизацией существующих решений, разработкой новых, исправлением ошибок, внедрением доработок. Роль человека в цифровой экономике минимизируется, многие процессы автоматизируются. Для совершения трансформации разрабатываются и применяются новые информационные технологии. Все они обладают определенной значимостью и новизной, но не все являются революционными.

Что же такое революционная или значимая технология? К значимым технологиям относят те технологии, которые привносят принципиально новый этап развития нескольких отраслей. Например, электричество позволило развивать промышленность в десятки раз быстрее, чем это было ранее, позволило появиться тысячам изобретений, которые без электричества просто были бы бессмысленны или нереальны. К значимой технологии относится Интернет. С его появлением началось бурное развитие дистанционных технологий, обмен информацией стал производиться практически мгновенно, у людей появилась возможность общения со всем миром.

С развитием Интернет возникли проблемы доверия между сторонами. Все, наверное, помнят карикатуру о двух собаках перед компьютером, где одна из них говорит другой: «В Интернете никто не знает, что ты – собака». Анонимность и отсутствие доверия сдерживает развитие многих процессов, необходимых во множестве отраслей

[](https://www.google.ru/url?sa=i&rct=j&q=&esrc=s&source=imgres&cd=&cad=rja&uact=8&ved=2ahUKEwis4ZX43KHfAhWLCCwKHXT4BhMQjRx6BAgBEAU&url=https%3A%2F%2Fen.wikipedia.org%2Fwiki%2FOn_the_Internet%2C_nobody_knows_you%2527re_a_dog&psig=AOvVaw1FLpItVKS_iBJ3nqRrMetL&ust=1544959541502708)

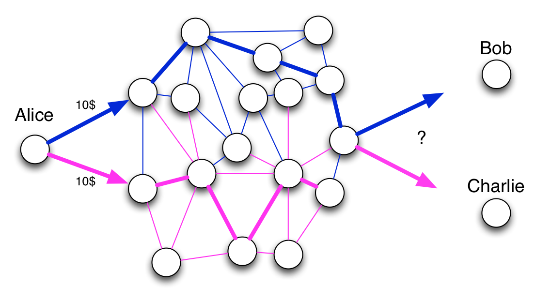
Перед человечеством стоит задача создания доверенной системы управления ценностями и блокчейн является одной из технологий, с помощью которой пытаются ее решить.



Итак, в чем же новшество технологии блокчейн и какие задачи она решает?

Сети P2P, как и другие распределенные системы, столкнулись с решением сложной проблемы, которая отсутствовала в реляционных базах данных: решение конфликтов и согласованность. Если в сети одновременно возникают два несовместимых факта, система должна иметь четкий алгоритм, какой факт признать верным.

Ярким примером несовместимых фактов является проблема двойной траты



У Alice есть всего $10. Alice одновременно пытается отправить $10 двум получателям. Как система должна определить, кому достанутся деньги и должна ли она провести транзакцию по обоим получателям? Для того, чтобы ответить на этот вопрос, необходимо упорядочить факты. Если в сеть поступают два несовместимых факта, то выигрывать должен тот факт, которые поступил первым. Но что же делать, если факты отправлены практически одновременно на отдаленных узлах сети? Как можно добиться согласованности всей сети с первым фактом? Именно этот вопрос был решен применением *алгоритма консенсуса* в децентрализованных сетях. Консенсусные алгоритмы необходимы для обеспечения достоверности транзакций через проверку точности приведенных действий. Именно это является особенностью блокчейна.

Как же отнеслось общество к появлению новой технологии? Несмотря на то, что блокчейн криптовалюты Биткойн был запущен в 2009 году, многие не обращали на него внимание почти пять лет. Часто блокчейн связывают только с миром криптовалют, забывая о его характеристиках и преимуществах.

Главным преимуществом блокчейна является то, что с его помощью можно исключить бюрократическую волокиту и автоматизировать множество бумажных процессов, увеличить доверие между сторонами без привлечения третьих лиц.

В целом отношение к блокчейну со стороны общества можно назвать настороженно-восторженным. Происходит это по следующим причинам:

1. Однажды созданную сеть невозможно взять под контроль властей, ее невозможно изменить или заблокировать/закрыть. Люди доверяют независимым системам, хотя в большинстве случаев не представляют, как эти системы работают.
2. Большинство людей в мире живут с нестабильными политическими и финансовыми системами, с дорогими финансовыми услугами низкого качества и шаткой национальной валютой. Использование криптовалют сделало возможным международные торговые сделки в таких странах, дало уверенность и чувство финансовой защищенности.
3. Несмотря на то, что объем криптовалют составляет примерно 1% объема мировых денег, наблюдается устойчивая тенденция роста как объемов криптовалют, так и их курса.

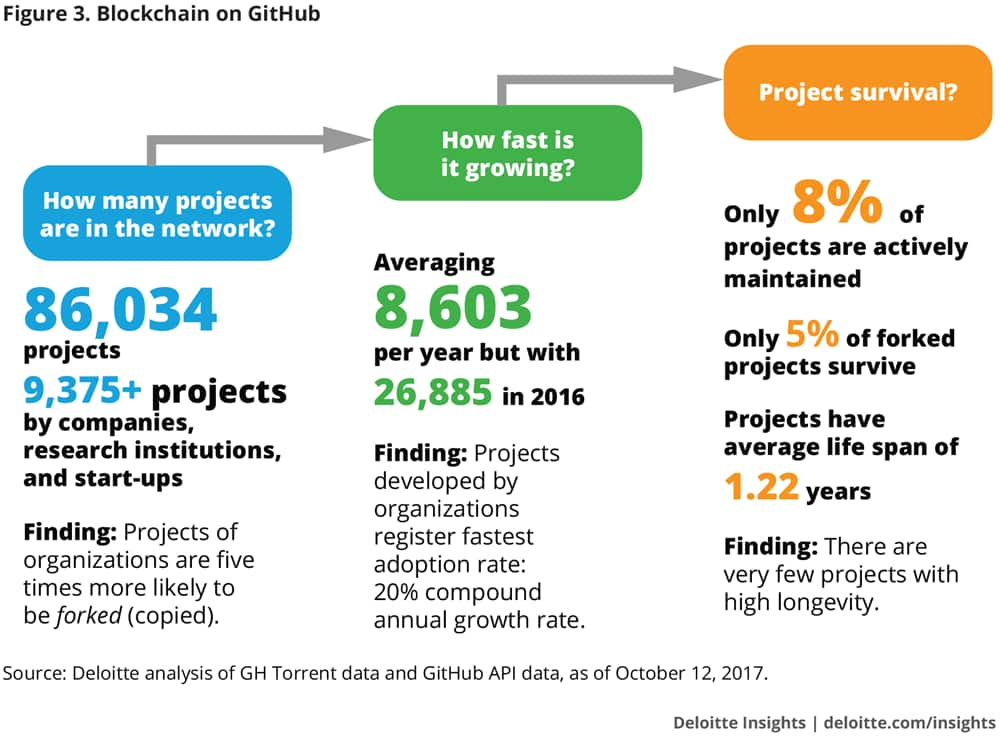
Итак, какие же изменения ждать от применения блокчейна?

Смарт-контракты – специальные компьютерные протоколы, позволяющие выполнять надежные транзакции без третьих сторон - помогут четко сформулировать правила взаимодействия, правила взаиморасчетов и практически решат проблему урегулирования споров.

Криптовалюты контролируются децентрализованным сообществом, их эмиссия происходит в сетях, где нет центрального доверенного узла и исключают вмешательство в эмиссию какого-либо государства. В связи с тем, что передача криптовалют необратима — никто не может отменить, заблокировать, оспорить или принудительно (без приватного ключа) совершить транзакцию, - ее использование в экономике и финансовом секторе сможет предотвратить мошенничество и внешнее вмешательство в сделки.

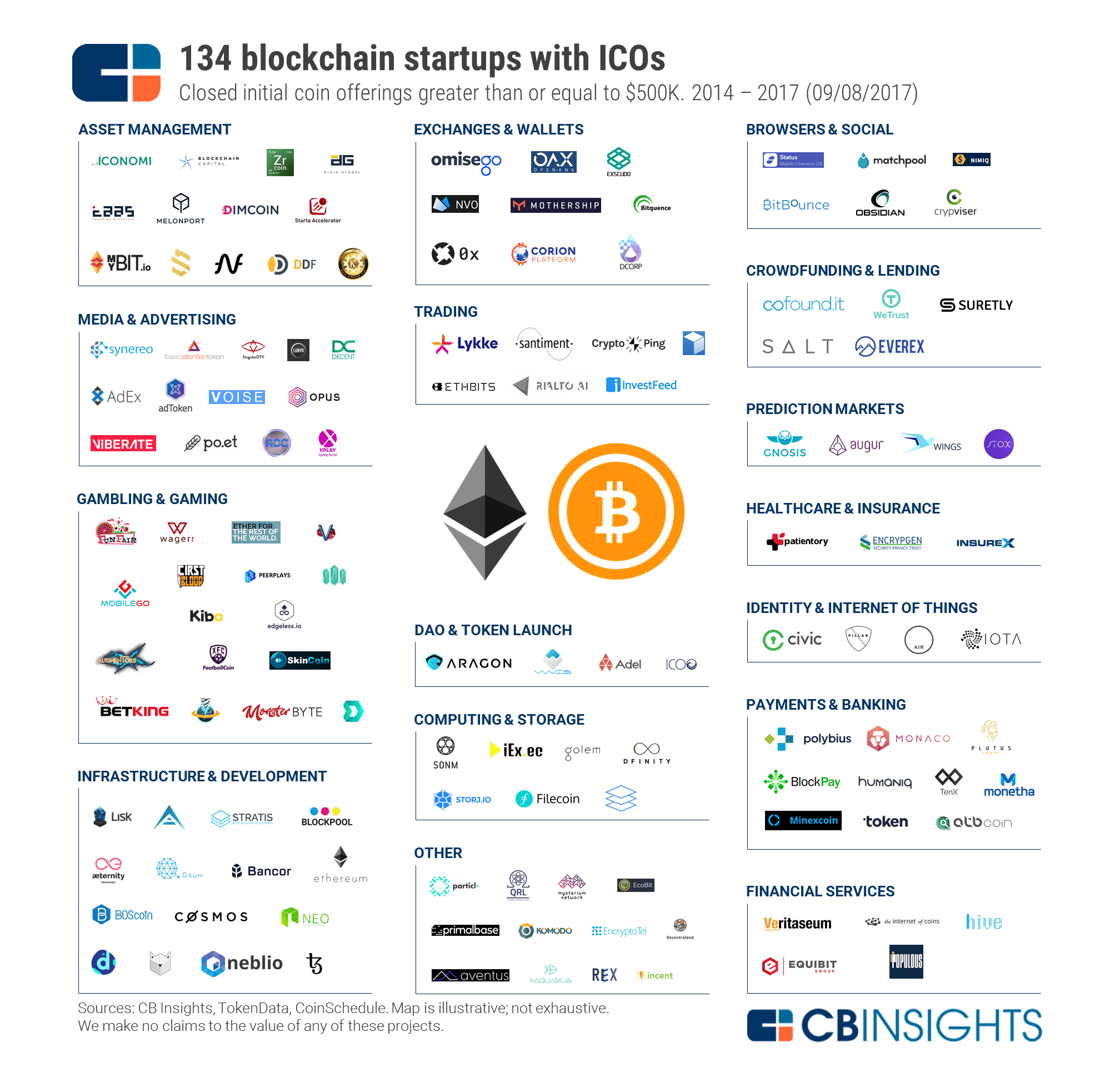
Многие крупные ИТ-компании разработали собственные блокчейны и решения. Успешные внедрения решений продемонстрировала компания IBM: ее решения на базе блокчейна внедрены в FedEx (система отслеживания грузов), совместно с Walmart IBM создала блокчейн-альянс продуктовой безопасности. Также разработаны самостоятельные решения не требующие внедрения в структуру компании.

Начиная 2016 года наблюдается бурный рост количества проектов, созданных на базе блокчейна. Однако большинство проектов оказывается нежизнеспособными по ряду причин: непродуманность проекта, невостребованность проекта рынком, изначальное желание собрать деньги, не развивая проект и т.д.



Финансирование блокчейн проектов часто ведеся через ICO (Initial Coin Offering) – выпуск проектом купонов (токенов) предназначенных для оплаты услуг площадки с использованием криптовалюты в будущем. В отличие от IPO, покупатели валюты не получают доли в компании и никак не могут воздействовать на внутренние управленческие решения. На самом деле ICO —это ещё одна реализация модели краудфандинга, когда участники финансируют развитие компании сейчас для того, чтобы получить от неё какие-то блага в будущем.

Повышенный интерес к проектам вызывает широта применения технологии и ее очевидные преимущества.



https://www.cbinsights.com/research/report/blockchain-trends-opportunities/

Перед началом разработки проекта необходимо иметь четкое представление о том, в какой отрасли проект найдет свое применение. Необходимо определить тот круг лиц, кто будет пользоваться продуктом или сервисом, понять их потребности. Ниже приведены примеры использования технологии блокчейн в различных отраслях.

**Для бизнеса** использование блокчейна и криптовалют открывает множество возможностей. Во-первых, блокчейн упростит доступ к финансовым услугам жителям развивающихся стран, упростит ведение бухгалтерии и взаиморасчетов, улучшит взаимоотношение с финансовыми регуляторами и повысит качество финансовых операций. Во-вторых, он даст возможность быстрого роста стартапам и компаниям, благодаря умным контрактам улучшится и ускорится взаимоотношение как с партнерами, так и с контролирующими органами.

**В финансовом и банковском секторе** блокчейн окажет большое влияние на управление активами и пассивами, регулирование, риск-менеджмент, корпоративные финансы, управление счетами в обслуживании клиентов, торговые операции, процесс встречных сделок. Поможет значительно сэкономить финансы и время. Не за горами появление систем Open Banking. Компании Intel и Microsoft работают над созданием новой блокчейн-платформы CocoFramework для корпоративных клиентов. В платформу будут интегрированы расширения Intel® SoftwareGuardExtensions(Intel® SGX), которые обеспечивают дополнительные уровни защиты личных и конфиденциальных данных благодаря шифрованию данных об операциях, что также повышает масштабируемость. Помимо этого, новая платформа обещает повысить скорость проведения операций и позволит разработчикам создавать гибкие распределенные реестры, с которыми будет удобно работать компаниям.

В **медицине и страховании** применение блокчейна позволит оценивать страховые риски и заключать договора с использованием смарт-контрактов, вести историю болезни, доступную в любой точке мира, отслеживать цепочку поставок препаратов.

**В инфраструкутруре** блокчейн может быть применен при создании умных городов: в управлении ЖКХ, обеспечении безопасности сетей, взаиморасчетах, при подтверждении права владения и т.д

Наиболее перспективным я считаю использование блокчейна совместно с **IoT (Internet of Things)**. Благодаря смарт-контрактам возникнет огромный потенциал автоматизации большинства современных процессов во всех областях: начиная от домохозяйств и заканчивая атомными станциями.

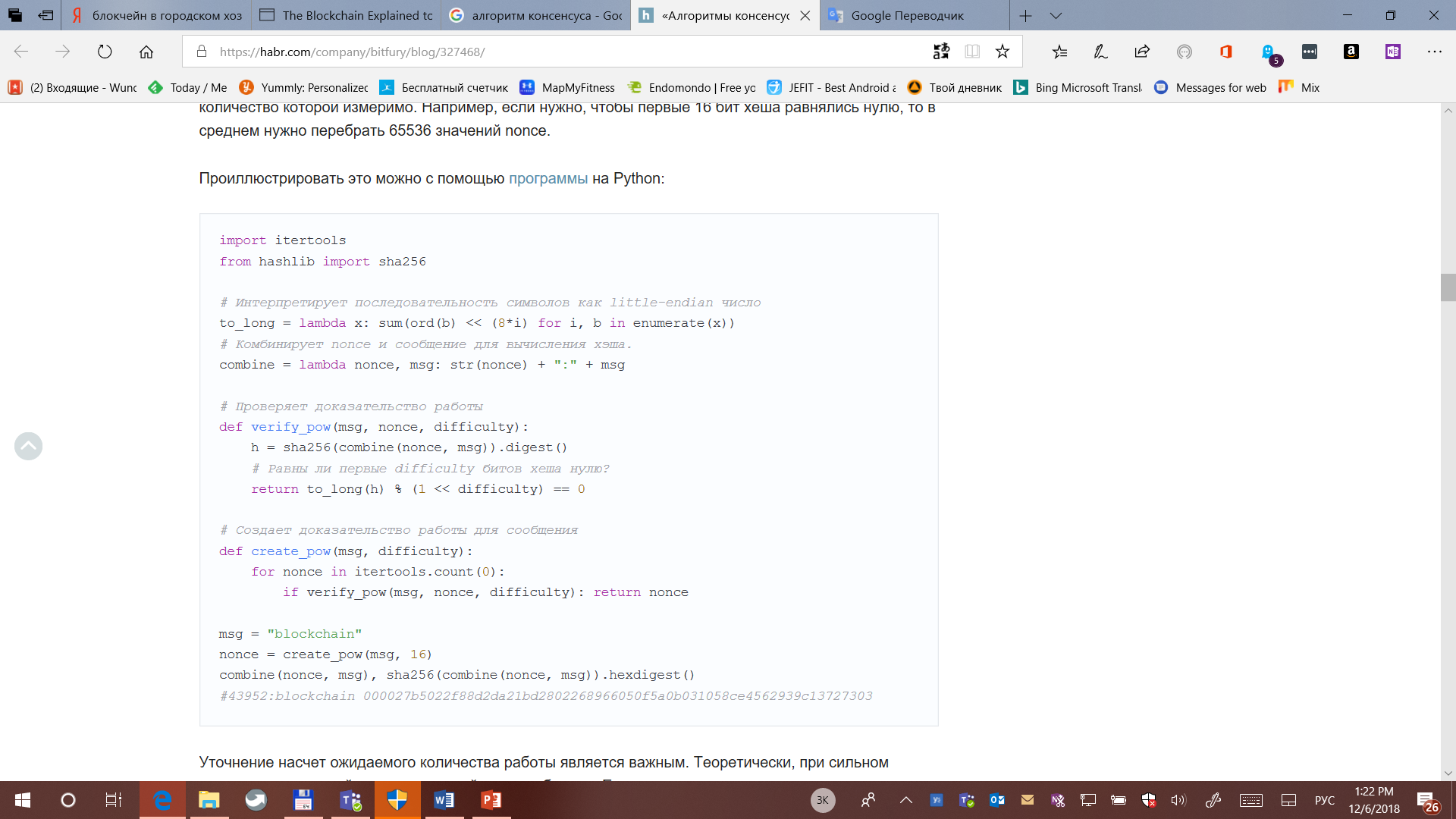
Глава 2. Как работает блокчейн, платформы для разработки приложений.

Блокчейн представляет собой распределенную децентрализованную систему, в которой могут находиться десятки тысяч участников. В основе взаимодействия сети заложен алгоритм консенсуса. Консенсус помогает решить вопрос достижения одинаковой точки зрения на журнал транзакций блокчейна в распределенной сети при условии, что произвольные узлы могут «падать» или зависать, руководствуясь лишь общими правилами обработки сообщений в сети. Идея консенсуса не нова и имеет реализованные решения в других распределенных системах (например, база данных NoSQL). Задача византийского консенсуса, в котором узлы могут вести себя «плохо» была сформулирована в 80-х годах прошлого века и уже имеет ряд решений. Консенсус в блокчейне отличается тем, что участники сети заранее неизвестны (в отличие от византийского консенсуса, у узлов которого есть «личности»), могут подключаться и отключаться от сети произвольно, блокчейн обладает объективностью (для определения текущей версии журнала транзакций не нужно доверие неким авторитетным источникам — корень доверия находится в самом блокчейне) и отсутствием регуляторов (никто не может вмешаться в работу сети).

Для технологии блокчейн разработано около десяти видов алгоритмов консенсуса. Рассмотрим их отличительные особенности

Proof-of-Work(PoW) - узлы блокчейн сети, подтверждающие транзакции проделывают достаточно сложную вычислительную работу (просчет алгоритма), результат работы легко и быстро проверяется другими узлами сети.Первый узел, который полностью провел все необходимые вычисления — получает вознаграждение от блокчейн сети. Все узлы борются между собой (наращивая емкость вычислительных ресурсов), чтобы оказаться тем самым, первым узлом, получившим вознаграждение. Основной недостаток – огромные энергетические затраты, т.к. работает множество узлов, а принимается результат работы только одного узла.

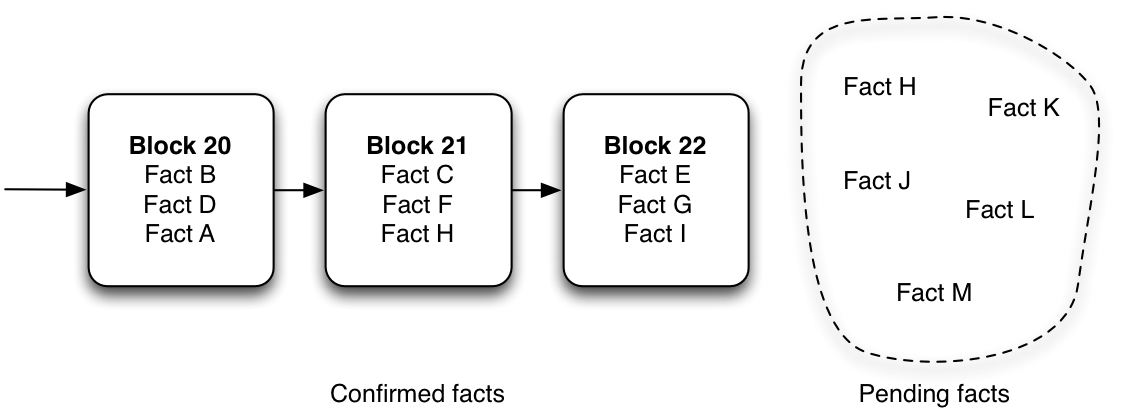
Пример алгоритма PoW, реализованного на Python ниже.



Proof-of-Stake (PoS). В этом алгоритме создателем следующего блока в цепочке блоков выбирается узел, который обладает б*о*льшим балансом — количеством ресурсов, например монет в криптовалюте. За само создание блока, узел вознаграждение не получает. Вознаграждение выплачивается за проведение транзакции. Основной недостаток – концентрация средств, которая может привести к централизации.

Помимо вышеперечисленных алгоритмов консенсуса, которые нашли широкое применение, также существуют алгоритмы, не менее перспективные, но используемые реже: Delegated PoS, Leased PoS, Proof-of-Capacity, Proof-of-Importance, Proof-of-Activity, Proof-of-Authority.

В любом блокчейне обрабатываются лишь два типа сообщений – транзакции и блоки, представляющие собой списки транзакций. Транзакции формируются участниками системы. Для формирования и отправки транзакций, например, таких как отправка криптовалюты участником сети, никаких алгоритмов не надо, достаточно использование ключа. Блоки являются основным продуктом алгоритма консенсуса и определяют порядок включения транзакций в журнал транзакций. Идея проста: факты (транзакции) группируются в блоки, и существует только одна цепочка блоков, реплицированных во всей сети. Каждый блок ссылается на предыдущий. Таким образом, если факт F находится в блоке 21, а факт E находится в блоке 22, то факт E рассматривается всей сетью как дочерний по отношению к факту F. Прежде, чем добавиться к блоку, факты находятся на рассмотрении, то есть до добавления они остаются неподтвержденными.



Теоретически, можно обойтись и без использования блоков, включая транзакции в журнал по отдельности. На практике блоки экономят объем трафика и вычислительные ресурсы сети.

Блоки создаются особой категорией узлов сети блокчейна – узлами консенсуса. Во многих блокчейнах (Bitcoi, Ethereum) эти узлы называют майнерами и они получают вознаграждение за свою работу, или комиссию. Майнеры соревнуются за то, чтобы их блок включили в сеть, т.к. только после проверки всеми узлами и включения блока в блокчейн все факты, находящиеся в блоке становятся подтвержденными и майнер получает свое вознаграждение. В некоторых блокчейнах майнеры также могут получать комиссию, которая приплюсовывается к вознаграждению.

Второй тип узлов сети блокчейн — это узлы аудита. Они имеют у себя полную копию блокчейна и не участвуют в процессе консенсуса. «Аудиторы» регулярно проверяют работу майнеров и занимаются распределением нагрузки по сети, выполняя функцию своеобразной сети доставки контента (CDN) для данных блокчейна.   
  
Третий тип узлов — это легкие клиенты, не имеющие полной версии блокчейна. Они содержат лишь важные для узла данные. Легкие клиенты требуют меньше вычислительных ресурсов и объемов памяти, поэтому могут работать на мобильных платформах.

